What is Claimed:

1. An information processing apparatus for converting message information from a first format into a second format, comprising:

a first cipher unit having a first cipher key input and a data output for outputting a data stream generated dependent on a first cipher key input via said first cipher key input,

a second cipher unit having a plaintext input a second cipher key input and a ciphertext output said second cipher unit via said cipher key input being communicatively coupled to said data output of the first cipher unit for receiving a second cipher key in the shape of said data stream; and

said first cipher unit being arranged to perform, dependent on a predetermined rule, a renewed generation of a data stream for use as said second cipher key.

2. An information processing apparatus as recited in claim 1, further being arranged to perform said renewed generation of a data stream for each occasion of key output.

3. An information processing apparatus as recited in claim 1, further comprising a synchronizing mechanism between the first and the second cipher unit being devised such that a renewed generation of a data stream is performed dependent on a synchronizing signal from the second cipher unit.

4. An information processing apparatus as recited in claim 1, further comprising a buffer for said data stream said buffer being arranged to output a data stream

stored in the buffer dependent on a synchronizing signal from the second cipher unit.

5. An information processing apparatus as recited in claim 1, further comprising a format adaptation mechanism devised to adapt said data stream to a format for a cipher key which is acceptable to said second cipher unit.

6. An information processing apparatus as recited in claim 1, wherein said second cipher unit is arranged to generate a block cipher.

7. An information processing apparatus as recited in claim 1, further being arranged to adapt said data stream to a format adapted to a cipher system that is arranged to generate a block cipher.

8. An information processing apparatus as recited in claim 1, wherein said second cipher unit is arranged to generate a stream cipher.

9. An information processing apparatus as recited in claim 1, further being arranged to adapt said data stream to a format adapted to a cipher system being arranged to generate a stream cipher.

10. An information processing apparatus as recited in claim 1, wherein said second cipher unit is arranged to generate encryption in accordance with DES.

11. An information processing apparatus as recited in claim 1, further being arranged to adapt said data stream to a format adapted to a cipher system being arranged to perform encryption in accordance with DES.

12. An information processing apparatus as recited in claim 1, wherein said second cipher unit is arranged to perform encryption in accordance with AES.

13. An information processing apparatus as recited in claim 1, further being arranged to adapt said data stream to a format adapted to a cipher system being arranged to perform encryption in accordance with AES.

14. An information processing apparatus as recited in claim 1, wherein said second cipher unit is arranged to perform encryption in accordance with the requirements in GSM, for example A5/1 or A5/2.

15. An information processing apparatus as recited in claim 1, further being arranged to adapt said data stream to a format adapted to a cipher system arranged to perform encryption in accordance with the requirements in GSM, for example A5/1 or A5/2.

16. An information processing apparatus for converting message information from a first format into a second format, comprising:

a first cipher unit having a first cipher key input and a data output for outputting a data stream generated dependent on a first cipher key input via said first cipher key input said first cipher unit comprising a memory for storage of data, means for updating said memory with input information, an instruction table having a set of operations arranged to modify the state of said memory, processing means arranged to select operations from said instruction table dependent on at least parts of said input information, and to execute said selected operations on the content of said memory wherein at least one of said set of operations is selectable dependent on every possible configuration of at least parts

of said input information, and means for extracting output information from said memory ,

a second cipher unit having a plaintext input a second cipher key input and a ciphertext out said second cipher unit via said second cipher key input being communicatively coupled to said data output of the first cipher unit for receiving a second cipher key in the shape of said data stream; and

said first cipher unit being arranged to perform, dependent on a predetermined rule, a renewed generation of a data stream for use as said second cipher key.

17. An information processing apparatus as recited in claim 16, further being arranged to perform said renewed generation of a data stream for each occasion of key output.

18. An information processing apparatus as recited in claim 16, further comprising a synchronizing mechanism between the first and the second cipher unit being devised such that a renewed generation of a data stream is performed dependent on a synchronizing signal from the second cipher unit.

19. An information processing apparatus as recited in claim 16, further comprising a buffer for said data stream said buffer being arranged to output a data stream stored in the buffer dependent on a synchronizing signal from the second cipher unit.

20. An information processing apparatus as recited in claim 16, further comprising a format adaptation mechanism devised to adapt said data stream to a format for a cipher key which is acceptable to said second cipher unit.

21 An information processing apparatus as recited in claim 16, wherein said second cipher unit is arranged to generate a block cipher.

22. An information processing apparatus as recited in claim 16, further being arranged to adapt said data stream to a format adapted to a cipher system that is arranged to generate a block cipher.

23. An information processing apparatus as recited in claim 16, wherein said second cipher unit is arranged to generate a stream cipher.

24. An information processing apparatus as recited in claim 16, further being arranged to adapt said data stream to a format adapted to a cipher system being arranged to generate a stream cipher.

25. An information processing apparatus as recited in claim 16, wherein said second cipher unit is arranged to generate encryption in accordance with DES.

26. An information processing apparatus as recited in claim 16, further being arranged to adapt said data stream to a format adapted to a cipher system being arranged to perform encryption in accordance with DES.

27. An information processing apparatus as recited in claim 16, wherein said second cipher unit is arranged to perform encryption in accordance with AES.

28. An information processing apparatus as recited in claim 16, further being

arranged to adapt said data stream to a format adapted to a cipher system being arranged to perform encryption in accordance with AES.

29. An information processing apparatus as recited in claim 16, wherein said second cipher unit is arranged to perform encryption in accordance with the requirements in GSM, for example A5/1 or A5/2.

30. An information processing apparatus as recited in claim 16, further being arranged to adapt said data stream to a format adapted to a cipher system arranged to perform encryption in accordance with the requirements in GSM, for example A5/1 or A5/2.

31. An information processing apparatus as recited in claim 16, further comprising a feedback unit coupled to said memory and arranged to combine a first processing material with a processing material obtained from a previous processing step, to feedback processing material to a program memory and to output a data stream in the shape of a completed internal key.

32. An information processing apparatus as recited in claim 31, wherein the feedback unit comprises a feedback memory, possibly realized as a stack, coupled to a functional unit having a feedback to the feedback memory and to the output of the feedback unit according to a predetermined function.

33. An information processing apparatus as recited in claim 32, wherein the functional unit comprises a linear feedback and/or a non-linear feedback.

34. An information processing apparatus as recited in claim 32, wherein the functional unit comprises a select operator a plurality of operators coupled to memory outputs and an addition operator coupled to the operators, wherein the select operator is arranged to select an operator dependent on a predetermined rule.

35. An information processing apparatus as recited in claim 16, wherein the memory comprises two memory units a cross connection unit and a second memory means having a control unit and a memory space arranged for storing status information of the memory units where any of the two firstly mentioned memory units is externally available and wherein it is arranged such that the content in said second memory means is exchangeable.

36. An information processing apparatus as recited in claim 35, wherein the cross connection unit is arranged such that both memory parts can be called simultaneously, and such that the memory parts are instantaneously interchangeable.

37. A computer implemented information processing method for converting message information from a first format into a second format, comprising the steps of:

a first encryption algorithm taking a first cipher key as an input and generating a data stream dependent on said first cipher key;

a second encryption algorithm taking plaintext as an input, taking a second cipher key as an input and generating a ciphertext dependent on said plaintext and on said second cipher key said second encryption algorithm receiving a second cipher key in the shape of said data stream from said first encryption algorithm; and

said first encryption algorithm performing, dependent on a predetermined rule, a renewed generation of a data stream for use as said second cipher key

38. An information processing method as recited in claim 37, further comprising the step of performing said renewed generation of a data stream for each occasion of key output.

39. An information processing method as recited in claim 37, further comprising the step of synchronizing the steps in the first and the second encryption algorithms such that the renewed generation of a data stream is performed dependent on a synchronizing parameter from the second encryption algorithm.

40. An information processing method as recited in claim 37, further comprising the steps of buffering said data stream and forwarding a stored data stream dependent on a synchronizing parameter from the second encryption algorithm.

41. An information processing method as recited in claim 37, further comprising the step of adapting said data stream to a format for a cipher key which is acceptable to said second encryption algorithm.

42. An information processing method as recited in claim 37, wherein said second encryption algorithm is arranged to generate a block cipher.

43. An information processing method as recited in claim 37, further comprising the step of adapting said data stream to a format adapted to an encryption algorithm that is arranged to generate a block cipher.

44. An information processing method as recited in claim 37, wherein said second encryption algorithm is arranged to generate a stream cipher.

45. An information processing method as recited in claim 37, further comprising the step of adapting said data stream to a format adapted to an encryption algorithm being arranged to generate a stream cipher.

46. An information processing method as recited in claim 37, wherein said second encryption algorithm is arranged to generate encryption in accordance with DES.

47. An information processing method as recited in claim 37, further comprising the step of adapting said data stream to a format adapted to an encryption algorithm being arranged to perform encryption in accordance with DES.

48. An information processing method as recited in claim 37, wherein said second encryption algorithm is arranged to perform encryption in accordance with AES.

49. An information processing method as recited in claim 37, further comprising the step of adapting said data stream to a format adapted to an encryption algorithm being arranged to perform encryption in accordance with AES.

50. An information processing method as recited in claim 37, wherein said second encryption algorithm is arranged to perform encryption in accordance with the requirements in GSM, for example A5/1 or A5/2.

51. An information processing method as recited in claim 37, further comprising the step of adapting said data stream to a format adapted to an encryption algorithm arranged to perform encryption in accordance with the requirements in GSM,

for example A5/1 or A5/2.

52. A computer implemented information processing method for converting message information from a first format into a second format, comprising the steps of:

a first encryption algorithm including the steps of establishing a set of operations arranged for modifying the state of a memory, storing input information in a first format in said memory, selecting operations from said set of operations dependent on at least parts of said input information, and executing said selected operations on the content of said memory, wherein at least one of said set of operations is selectable dependent on every possible configuration of said input information, and extracting information from said memory in a second format after the execution of at least one operation;

a second encryption algorithm taking plaintext as an input, taking a second cipher key as an input and generating a ciphertext dependent on said plaintext and on said second cipher key said second encryption algorithm receiving a second cipher key in the shape of said data stream from said first encryption algorithm; and

said first encryption algorithm performing, dependent on a predetermined rule, a renewed generation of a data stream for use as said second cipher key.

53. An information processing method as recited in claim 52, further comprising the step of performing said renewed generation of a data stream for each occasion of key output.

54. An information processing method as recited in claim 52, further comprising the step of synchronizing the steps in the first and the second encryption algorithms such that the renewed generation of a data stream is performed dependent on a synchronizing parameter from the second encryption algorithm.

55. An information processing method as recited in claim 52, further comprising the steps of buffering said data stream and forwarding a stored data stream dependent on a synchronizing parameter from the second encryption algorithm.

56. An information processing method as recited in claim 52, further comprising the step of adapting said data stream to a format for a cipher key which is acceptable to said second encryption algorithm.

57. An information processing method as recited in claim 52, wherein said second encryption algorithm is arranged to generate a block cipher.

58. An information processing method as recited in claim 52, further comprising the step of adapting said data stream to a format adapted to an encryption algorithm that is arranged to generate a block cipher.

59. An information processing method as recited in claim 52, wherein said second encryption algorithm is arranged to generate a stream cipher.

60. An information processing method as recited in claim 52, further comprising the step of adapting said data stream to a format adapted to an encryption algorithm being arranged to generate a stream cipher.

61. An information processing method as recited in claim 52, wherein said second encryption algorithm is arranged to generate encryption in accordance with DES.

62. An information processing method as recited in claim 52, further

comprising the step of adapting said data stream to a format adapted to an encryption algorithm being arranged to perform encryption in accordance with DES.

63. An information processing method as recited in claim 52, wherein said second encryption algorithm is arranged to perform encryption in accordance with AES.

64. An information processing method as recited in claim 52, further comprising the step of adapting said data stream to a format adapted to an encryption algorithm being arranged to perform encryption in accordance with AES.

Rule 1.126

65 ~~66.~~ An information processing method as recited in claim 52, wherein said second encryption algorithm is arranged to perform encryption in accordance with the requirements in GSM, for example A5/1 or A5/2.

66 ~~67.~~ An information processing method as recited in claim 52, further comprising the step of adapting said data stream to a format adapted to an encryption algorithm arranged to perform encryption in accordance with the requirements in GSM, for example A5/1 or A5/2.

67 ~~68.~~ An information processing method as recited in claim 52, further comprising the steps of combining, in a feedback stage, a first processing material with a processing material obtained from a previous processing step, feeding back processing material to a program memory and outputting a data stream in the shape of a completed internal key.

68 ~~69.~~ An information processing method as recited in claim 67, wherein the feedback stage comprises a linear feedback and/or a non-linear feedback.

69

~~70.~~ An information processing method as recited in claim 67, further comprising the step of selecting a function operator from a plurality of operators dependent on a predetermined rule.

Rule 1.126

70

~~71.~~ An information processing method as recited in claim 67, further comprising the steps of initializing said memory in the shape of two memory units, cross connecting said memory units to the memory output and to a second memory means, storing status information of the memory units in another memory space, wherein any of the two firstly mentioned memory units is externally available and wherein it is arranged such that the content in said second memory means is exchangeable.

71

~~72.~~ An information processing method as recited in claim 70, wherein the cross connection is arranged such that both memory parts can be called simultaneously, and such that the memory parts are instantaneously interchangeable.

72

~~73.~~ A computer program product, for use in a data processing system, for converting message information from a first format into a second format, comprising program code for directing the data processing system:

to perform a first encryption algorithm taking a first cipher key as an input and generating a data stream dependent on said first cipher key ;

to perform a second encryption algorithm taking plaintext as an input, taking a second cipher key as an input and generating a ciphertext dependent on said plaintext and on said second cipher key said second encryption algorithm receiving a second cipher key in the shape of said data stream from said first encryption algorithm; and

to perform by means of said first encryption algorithm and, dependent on a predetermined rule, a renewed generation of a data stream for use as said second cipher key.

73

74. A computer program product as recited in claim 72, further comprising program code for directing the data processing system to perform said renewed generation of a data stream for each occasion of key output.

74

75. A computer program product as recited in claim 72, further comprising program code for directing the data processing system to synchronize the steps in the first and the second encryption algorithms such that the renewed generation of a data stream is performed dependent on a synchronizing parameter from the second encryption algorithm.

Rule 1.126

75

76. A computer program product as recited in claim 72, further comprising program code for directing the data processing system to buffer said data stream and to forward a stored data stream dependent on a synchronizing parameter from the second encryption algorithm.

76

77. A computer program product as recited in claim 72, further comprising program code for directing the data processing system to adapt said data stream to a format for a cipher key which is acceptable to said second encryption algorithm.

77

78. A computer program product as recited in claim 72, wherein said second encryption algorithm is arranged to generate a block cipher.

78

79. A computer program product as recited in claim 72, further comprising program code for directing the data processing system to adapt said data stream to a format adapted to an encryption algorithm that is arranged to generate a block cipher.

79

80. A computer program product as recited in claim 72, wherein said second encryption algorithm is arranged to generate a stream cipher.

80

81. A computer program product as recited in claim 72, further comprising program code for directing the data processing system to adapt said data stream to a format adapted to an encryption algorithm being arranged to generate a stream cipher.

81

82. A computer program product as recited in claim 72, wherein said second encryption algorithm is arranged to generate encryption in accordance with DES.

82

83. A computer program product as recited in claim 72, further comprising program code for directing the data processing system to adapt said data stream to a format adapted to an encryption algorithm being arranged to perform encryption in accordance with DES.

83

84. A computer program product as recited in claim 72, wherein said second encryption algorithm is arranged to perform encryption in accordance with AES.

84

85. A computer program product as recited in claim 72, further comprising program code for directing the data processing system to adapt said data stream to a format adapted to an encryption algorithm being arranged to perform encryption in accordance with AES.

85

86. A computer program product as recited in claim 72, wherein said second encryption algorithm is arranged to perform encryption in accordance with the requirements in GSM, for example A5/1 or A5/2.

86
87. A computer program product as recited in claim 72, further comprising program code for directing the data processing system to adapt said data stream to a format adapted to an encryption algorithm arranged to perform encryption in accordance with the requirements in GSM, for example A5/1 or A5/2.

87
88. A computer program product for converting message information from a first format into a second format, comprising program code for directing the data processing system:

to perform a first encryption algorithm including the steps of establishing a set of operations arranged for modifying the state of a memory, storing input information in a first format in said memory, selecting operations from said set of operations dependent on at least parts of said input information, and executing said selected operations on the content of said memory, wherein at least one of said set of operations is selectable dependent on every possible configuration of said input information, and extracting information from said memory in a second format after the execution of at least one operation;

to perform a second encryption algorithm taking plaintext as an input, taking a second cipher key as an input and generating a ciphertext dependent on said plaintext and on said second cipher key said second encryption algorithm receiving a second cipher key in the shape of said data stream from said first encryption algorithm; and

to perform, by means of said first encryption algorithm and dependent on a predetermined rule, a renewed generation of a data stream for use as said second cipher key.

88
89. A computer program product as recited in claim 87, further comprising program code for directing the data processing system to perform said renewed generation of a data stream for each occasion of key output.

89

~~90.~~ A computer program product as recited in claim 87, further comprising program code for directing the data processing system to synchronize the steps in the first and the second encryption algorithms such that the renewed generation of a data stream is performed dependent on a synchronizing parameter from the second encryption algorithm.

Rule 1.126

90

~~91.~~ A computer program product as recited in claim 87, further comprising program code for directing the data processing system to buffer said data stream and to forward a stored data stream dependent on a synchronizing parameter from the second encryption algorithm.

91

~~92.~~ A computer program product as recited in claim 87, further comprising program code for directing the data processing system to adapt said data stream to a format for a cipher key which is acceptable to said second encryption algorithm.

92

~~93.~~ A computer program product as recited in claim 87, wherein said second encryption algorithm is arranged to generate a block cipher.

93

~~94.~~ A computer program product as recited in claim 87, further comprising program code for directing the data processing system to adapt said data stream to a format adapted to an encryption algorithm that is arranged to generate a block cipher.

94

~~95.~~ A computer program product as recited in claim 87, wherein said second encryption algorithm is arranged to generate a stream cipher.

95

~~96.~~ A computer program product as recited in claim 87, further comprising program code for directing the data processing system to adapt said data stream to a format adapted to an encryption algorithm being arranged to generate a stream cipher.

Rule 1.126

96

~~97.~~ A computer program product as recited in claim 87, wherein said second encryption algorithm is arranged to generate encryption in accordance with DES.

97

~~98.~~ A computer program product as recited in claim 87, further comprising program code for directing the data processing system to adapt said data stream to a format adapted to an encryption algorithm being arranged to perform encryption in accordance with DES.

98

~~99.~~ A computer program product as recited in claim 87, wherein said second encryption algorithm is arranged to perform encryption in accordance with AES.

99

~~100.~~ A computer program product as recited in claim 87, further comprising program code for directing the data processing system to adapt said data stream to a format adapted to an encryption algorithm being arranged to perform encryption in accordance with AES.

100

~~101.~~ A computer program product as recited in claim 87, wherein said second encryption algorithm is arranged to perform encryption in accordance with the requirements in GSM, for example A5/1 or A5/2.

101

~~102.~~ A computer program product as recited in claim 87, further comprising program code for directing the data processing system to adapt said data stream to a

format adapted to an encryption algorithm arranged to perform encryption in accordance with the requirements in GSM, for example A5/1 or A5/2.

102

~~103.~~ A computer program product as recited in claim 87, further comprising program code for directing the data processing system to combine, in a feedback stage, a first processing material with a processing material obtained from a previous processing step, to feed back processing material to a program memory and to output a data stream in the shape of a completed internal key

103

~~104.~~ A computer program product as recited in claim 102, wherein the feedback stage comprises a linear feedback and/or a non-linear feedback.

104

~~105.~~ A computer program product as recited in claim 102, further comprising program code for directing the data processing system to select, for the feedback, a function operator from a plurality of operators dependent on a predetermined rule.

105

~~106.~~ A computer program product as recited in claim 102, further comprising program code for directing the data processing system to initialize said memory in the shape of two memory units, to cross connect said memory units to the memory output and to a second memory means, to store status information of the memory units in another memory space, wherein any of the two firstly mentioned memory units is externally available and wherein it is arranged such that the content in said second memory means is exchangeable.

106

~~107.~~ A computer program product as recited in claim 105, wherein the cross connection unit is arranged such that both memory parts can be called simultaneously, and such that the memory parts are instantaneously interchangeable.